

認証後に送り側(ソース機器)と受信側(シンク機器)とで共有した認証鍵により、52bitのコンテンツ鍵を生成する。コンテンツ鍵はCCIにより異なり、時間と共に変化する時変鍵となっている。これにより暗号強度を高めている。

■ 家中どこでもAVネット

DTCPはDTCP-IPへと更なる発展を遂げた。家庭内ネットワーク(LAN)への対応だ。LANの通信プロトコルTCP-IPへ対応することで、家庭内でLANに接続したパソコンや、Wi-Fi接続でスマホ、タブレットなどでもDTCP-IPに対応したハードディスクレコーダーに録画した動画を見たりできるようになった。

DTCP-IPではオープンな仕様のLANに、データをパケットと呼ぶ単位で送る。そのため、認証は完全認証として、伝送時にはデータを常に暗号化することになった。このパケットをPCP(Protected Content Packet:保護されたコンテンツパック)と呼ぶ。暗号化のアルゴリズムには共通鍵暗号で鍵サイズが128bitのAES(AES-128)が採用された。

AKE(認証及び鍵共有)の手順はDHCPと変わらないが、CCIはこのPCPのヘッダ部4bitのE-EMI(Extended Encryption Mode Indicator)領域に保存される。4bit化することでCCIは以下のように拡張された。

▼ DTCP-IP の PCP 構造

